PERSPEKTIF & PANDANGAN GLOBAL

Inovasi dan Teknologi

BAGIAN I: Peran Audit Internal di Dalam Asurans Teknologi

BAGIAN II: Tetap Mengikuti Perkembangan Adopsi Teknologi Organisasi

BAGIAN III: Tantangan Mengenai Talenta Teknologi Audit Internal

Wolters Kluwer

The Institute of Internal Auditors

Contents

Diterjemahkan dan diselaraskan oleh IIA Indonesia Volunteer:

1. I Made Suandi Putra, CIA, CRMA
2. Fauzan Wahyuabdi Pratama, CIA, CGAP
3. Indra Permana, CIA, CRMA
4. Diana Laurencia Sidauruk, CIA
5. Riani Nurainah Lisnasari, CIA
6. I Gde Wiyadnya
7. Agnes Maria Widiyanti

Bagian 1: Peran Audit Internal di Dalam Asurans Teknologi

Tentang Ahli

Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, adalah manajer produk senior di TeamMate Audit Solutions, di mana dia bekerja untuk terus meningkatkan produktivitas audit sambil memberikan wawasan strategis melalui solusi TeamMate yang terbaik di kelasnya. Beliau memiliki lebih dari 20 tahun pengalaman audit internal baik di sektor publik maupun swasta.

Sebelumnya, Jim memegang sejumlah peran kepemimpinan di The Institute of Internal Auditors, menjabat sebagai Auditor Pemerintah Kota untuk Kota Palo Alto, CA, dan Kepala Audit untuk Wilayah San Diego, CA. Latar belakang audit internalnya yang beragam mencakup posisi di California State University System, PETCO Animal Supplies, Inc., State Street Corporation, dan General Electric.

Pendahuluan

Teknologi telah menjadi pendorong perubahan dan inovasi bisnis yang tidak perlu diragukan lagi. Dari transformasi digital yang meluas hingga kecerdasan artifisial yang muncul dan semakin berkembang, teknologi baru telah membuka peluang – dan risiko- yang belum pernah ada sebelumnya. Untuk memahami dampak teknologi baru, organisasi mengandalkan audit internal untuk mendapatkan asurans mengenai adopsi dan penggunaan teknologi oleh organisasi. Laporan ringkas ini akan mengulas mengapa asurans teknologi harus menjadi bagian rutin dari setiap audit. Laporan ini akan mencakup area-area kerentanan utama dan peluang bagi audit internal untuk memimpin pewujudan konsistensi dan koordinasi yang akan menghasilkan audit teknologi yang lebih efektif.

Sebuah fokus sentral

Karena teknologi telah menjangkau setiap aspek bisnis, wajar jika asurans terhadap teknologi sudah menjadi fokus sentral bagi para auditor internal. “Pada dasarnya terdapat risiko teknologi dalam segala hal yang dilaksanakan organisasi, kata Jim Pelletier, CIA, CGAP, manajer senior produk pada TeamMate Audit Solutions. Tidak ada lagi pemisahan antara operasional dengan teknologi karena teknologi mendukung operasional dan berbagai fungsi lainnya. Mengevaluasi dan memastikan pengendalian yang layak harus mencakup teknologi yang mendasari suatu proses. Sebagai contoh, ketika auditor internal melakukan audit terhadap akun utang – atau fungsi lain – dan sistemnya secara terpisah, fungsi dan sistem kini sepenuhnya saling terkait, kata Pelletier. “ Semua yang Anda audit melibatkan asurans teknologi pada tingkat tertentu.”

Isu-Isu untuk Dipertimbangkan

Risiko pihak ketiga dan tata kelola data

Mengenali area ancaman utama

Karena prevalensi teknologi, terdapat banyak hal yang perlu dipertimbangkan dalam menyediakan asurans teknologi. Bagian ini akan membahas beberapa area berisiko tinggi.

Hubungan dengan Pihak ketiga

Riset telah menunjukkan bahwa 98% organisasi secara global memiliki hubungan vendor dengan setidaknya satu pihak ketiga yang pernah mengalami pelanggaran dalam dua tahun terakhir. Perusahaan-perusahaan juga dapat dipengaruhi oleh koneksi hilir vendor. Sebanyak 50% organisasi memiliki hubungan tidak langsung dengan setidaknya 200 vendor pihak keempat yang baru saja dibobol.[1]

Ketergantungan dan keterkaitan organisasi yang luas kepada pihak ketiga merupakan risiko penting, terutama ketika terjadi masalah. Hubungan dengan pihak ketiga mungkin sangat rentan karena banyak yang salah berasumsi bahwa vendor mampu mengatasi seluruh risiko terkait dan tidak diperlukan peninjauan lebih lanjut terhadap upaya mereka atau bahwa pengawasan yang kurang ketat tersebut dirasa sudah cukup.

Contoh perusahaan yang telah mengalami kebocoran data pihak ketiga ini menunjukkan bahwa jenis organisasi atau industri apapun dapat terdampak: SolarWinds AT&T, Chick-fil-A, LinkedIn, T-Mobile, Uber, Okta, dan Dollar Tree.[2]

Teknologi atau layanan terkait yang disediakan vendor pihak ketiga bisa mencakup layanan platform *web-hosting* dan *software-as-a-service* (SaaS), pusat data yang dialihdayakan, atau keamanan jaringan. Ketika penyedia mengambil tanggung jawab terhadap layanan yang ditawarkannya, organisasi yang menggunakan layanan tersebut harus tetap memastikan bahwa mereka memiliki pengendalian dan proses manajemen risiko yang tepat untuk mengawasi bahwa pihak ketiga telah memenuhi kewajibannya. “Anda tidak dapat mendasarkan keamanan organisasi pada harapan bahwa pihak ketiga akan melaksanakan pekerjaan mereka,” kata Pelletier.

Auditor internal sebaiknya mempertimbangkan apakah organisasi mereka telah secara tepat mengevaluasi pihak ketiga dan risiko terkaitnya dengan benar. Auditor internal boleh tidak melaksanakan evaluasi ini, namun sebaiknya dipertimbangkan bagaimana organisasi memantau dan mengelola hubungan dan risiko terkaitnya, serta memverifikasi bahwa pihak ketiga telah memiliki dan melaksanakan pengendalian yang tepat. Pelletier merekomendasikan untuk menyertakan klausul hak untuk audit di dalam kontrak dengan vendor sehingga audit internal dapat memeriksa proses dan pengendalian vendor sesuai kebutuhan, termasuk setelah terjadi kebocoran.

Tata kelola data

Organisasi-organisasi mengumpulkan data dengan volume yang semakin bertumbuh secara cepat dan memanfaatkannya dengan teknologi terkini seperti kecerdasan artifisial. Data dapat menghadirkan risiko penting bagi organisasi karena pentingnya memelihara privasi data. Selain itu, jika pimpinan akan mengambil keputusan bisnis penting berbasis data yang ada, organisasi harus yakin terhadap integritas data dan memastikan data tersebut lengkap, akurat, dan dapat diandalkan. Hal ini termasuk memahami keandalan sumber data, utamanya ketika bekerja dengan kecerdasan artifisial generatif.

[1] “SecurityScorecard Research Shows 98% of Organizations Globally Have Relationships With At Least One Breached Third-Party,” SecurityScorecard press release based on a study by SecurityScorecard and The Cyentia Institute, February 1, 2022.
[2] “Top Third-Party Data Breaches in 2023,” FortifyData, updated December 4, 2023.

Organisasi akan perlu untuk menjamin bahwa data tidak rentan terhadap peretasan atau penggunaan tidak layak lainnya. "Organisasi perlu mengevaluasi bagaimana data diproses dan disimpan", kata Pelletier, serta memastikan bahwa persyaratan hukum atau regulasi yang spesifik telah dipenuhi, misalnya yang terkait dengan privasi informasi. Jika organisasi telah memberikan asurans kepada pelanggan atau mitra bisnis tentang bagaimana data mereka akan digunakan, ini perlu untuk memastikan bahwa komitmen tersebut dipenuhi. Meskipun manajemen bertanggung jawab terhadap tata kelola data, auditor internal dapat menawarkan asurans bahwa pengendalian tata kelola data telah memadai.

Data sebaiknya disimpan dalam jangka waktu yang sesingkat mungkin, menurut *European Commission*. Tidak hanya penyimpanannya yang mahal, namun juga, jika terjadi kejadian kebocoran, akan lebih banyak data yang dapat diakses oleh para peretas. Perusahaan sebaiknya memiliki aturan waktu yang tepat tentang kapan data sebaiknya ditinjau atau dihapus, dengan memperhatikan persyaratan bisnis, peraturan, dan legislatif yang mengharuskan periode retensi yang lebih lama untuk beberapa materi. Sebagai contoh, di bawah prinsip *General Data Protection Regulation* dari European Commission, komisi tersebut menunjuk suatu situasi di mana perusahaan penyimpan CV dari para pencari kerja selama 20 tahun, tanpa mengambil langkah untuk memperbaruinya. [3] Data ini jelas akan menjadi usang dalam waktu singkat, mengingat perputaran yang cepat pada pekerjaan dan industri. Orang tersebut mungkin akan kehilangan peluang pekerjaan dan perusahaan mungkin kehilangan orang berbakat jika mengandalkan pada kumpulan informasi yang usang ketika mencari pekerja untuk lowongan di masa mendatang, atau data pribadi pelamar mungkin dicuri jika organisasi diretas.

Beberapa area teknologi lain yang dapat diidentifikasi melalui asurans audit internal sebagai kegagalan organisasi dalam mengimplementasikan pemantauan atau perlindungan yang tepat meliputi:

- **Pengendalian akses**. Audit internal dapat memeriksa apakah reviu terhadap akses pengguna telah dilaksanakan untuk memastikan bahwa hanya pengguna yang sah yang memiliki akses ke dalam teknologi yang digunakan organisasi untuk bekerja. Selain itu, reviu yang dilakukan dapat mengidentifikasi apakah mantan pegawai atau anggota departemen memiliki akses yang tidak terotorisasi terhadap aplikasi atau infrastruktur, menurut Jurnal ISACA. "Kerentanan ini dapat dieksploitasi, sehingga mengakibatkan kerugian finansial atau reputasi bagi perusahaan," sebutnya.[4]
- **Keamanan siber**. "Penambalan keamanan, kata sandi yang kuat, manajemen aset, dan pelatihan keamanan bagi pegawai sangat membantu untuk tetap aman dalam lingkungan *online*," menurut artikel Forbes.[5]
- ***Shadow IT*.** Istilah ini mengacu pada situasi di mana pegawai membeli dan menerapkan teknologi tanpa sepengetahuan atau izin dari departemen TI. Praktik ini semakin berkembang seiring dengan meningkatnya pekerjaan jarak jauh dan meningkatnya penggunaan perangkat pribadi saat bekerja. Risikonya mencakup kegagalan untuk berada di bawah pengawasan tim TI atau kegagalan dalam mengikuti protokol keamanan siber dan privasi organisasi serta pedoman lainnya.
- **Risiko terkait kecerdasan artifisial generatif dan teknologi baru lainnya**. Bahaya bahwa karyawan dapat mengunggah data perusahaan, pelanggan, atau pribadi ke sistem kecerdasan artifisial generatif publik merupakan salah satu kekhawatiran yang signifikan. (Kerangka Kerja Audit Kecerdasan Artifisial dari Institute of Internal Auditors[6] membantu auditor internal memahami risiko dan menentukan praktik terbaik kecerdasan artifisial dan pengendalian internal.)
- **Pertimbangan kultur**. Auditor internal dapat mempertimbangkan apakah kurangnya keterlibatan karyawan atau buruknya komunikasi mengenai pedoman teknologi atau perlindungan merupakan suatu ancaman.
- **Dampak peraturan atau peraturan terkait teknologi.** Organisasi perlu memantau kebutuhan kepatuhan terkait peraturan undang-undang dan standar baru yang dikeluarkan sebagai respons terhadap perubahan signifikan yang dapat ditimbulkan oleh teknologi baru bagi bisnis dan masyarakat.

[3] "For how long can data be kept and is it necessary to update it?" European Commission.
[4] "Effective User Access Reviews," Sundaresan Ramaseshan, *ISACA Journal*, August 21, 2019.
[5] "16 Tech-Related Risk Factors Company Executives Often Overlook," *Forbes*, December 21, 2022.
[6] The Institute of Internal Auditors' AI Auditing Framework.

Nilai dari Upaya yang Terkoordinasi

Menyelaraskan dengan profesional risiko lini kedua

Audit internal dapat membantu mengoordinasikan manajemen risiko teknologi

Salah satu kelemahan dari kehadiran dan dampak teknologi yang meluas adalah risiko ada sesuatu yang akan diabaikan ketika mencoba untuk sepenuhnya memahami dan memberikan asurans pada bidang ini. "Karena ada begitu banyak hal yang harus ditutupi, maka akan ada kesenjangan," kata Pelletier. Mengingat banyaknya risiko yang terlibat, untuk meningkatkan efisiensi perannya sebagai penyedia asurans dalam adopsi dan penggunaan teknologi, audit internal ingin mendapatkan cakupan terbaik atas area berisiko tinggi dengan sumber daya yang tersedia.

Untuk meningkatkan sumber daya tersebut, fungsi audit internal memiliki peluang untuk menyelaraskan dengan fungsi asurans lini kedua seperti keamanan informasi, pengendalian internal, manajemen risiko, dan kepatuhan, menurut Pelletier. Untuk memberikan tingkat kenyamanan yang lebih tinggi bagi manajemen senior dan dewan ketika risiko diidentifikasi, audit internal dapat mengoordinasikan aktivitasnya dengan fungsi-fungsi ini untuk mendapatkan gambaran menyeluruh tentang bagaimana asurans teknologi – dan risiko teknologi utama – ditangani di seluruh organisasi.

Meskipun audit internal harus tetap independen terhadap fungsi-fungsi lini kedua ini, koordinasi dengan mereka dapat membantu audit internal menentukan risiko mana yang sudah ditanggung dan sejauh mana risiko tersebut. "Audit internal tidak boleh dilakukan secara terpisah," kata Pelletier. Dalam meminimalkan duplikasi upaya, penyelarasan memungkinkan audit internal memfokuskan sumber dayanya pada risiko yang paling penting. Sebagai bagian dari upaya tersebut, audit internal dapat mengevaluasi pekerjaan yang dilakukan fungsi lini kedua terkait dengan asurans teknologi.

Penyelarasan ini juga dapat membantu meminimalkan "kelelahan asurans", yang terjadi ketika banyak fungsi meminta manajer departemen untuk melaporkan data yang sama atau melakukan tinjauan serupa. Hal ini dapat dihindari jika audit internal dan fungsi lini kedua bekerja sama untuk mengumpulkan informasi inti yang mereka perlukan.

Audit internal dapat mengambil peran kepemimpinan dalam mengoordinasikan penyelarasan aktivitas asurans di seluruh organisasi dan memanfaatkan aktivitas yang ada dengan sebaik-baiknya, kata Pelletier. Sebagai permulaan, auditor internal dapat mendorong

Teknologi adalah hal utama bagi auditor internal

Teknologi menjadi fokus utama dalam *North American Pulse of Internal Audit* IIA 2023[7], yang mengumpulkan informasi tolok ukur yang berharga dari pimpinan audit internal mengenai risiko, rencana audit, anggaran, staf, dan topik hangat lainnya.

Misalnya, ketika *chief audit executive* ditanya bagaimana mereka akan membelanjakan uang anggaran tambahan jika mereka memilikinya, pilihan kedua yang paling umum adalah teknologi. (Peningkatan staf internal lebih diprioritaskan)

Meskipun peninjauan kepatuhan dan operasional merupakan prioritas tradisional, auditor internal juga menghabiskan banyak waktu dan upaya pada topik terkait teknologi. Dalam survei Pulse, responden mengatakan bahwa 10% dari rencana audit mereka berfokus pada keamanan siber dan 9% pada TI secara keseluruhan. Jumlah sebesar 19% ini lebih tinggi dari jumlah rata-rata rencana audit yang ditujukan untuk pelaporan keuangan (termasuk ICFR), operasional, dan kepatuhan/peraturan (tidak termasuk ICFR). Masing-masing dari mereka adalah subjek dari 15% rencana audit.

Terakhir, ketika responden diminta untuk memilih isu mana yang mempunyai risiko tinggi atau sangat tinggi bagi organisasi mereka, tiga pilihan teratas mereka semuanya berkaitan dengan teknologi:

- Keamanan siber, yang dipilih oleh 78% responden.
- TI secara keseluruhan, sebesar 57%.
- Hubungan dengan pihak ketiga, yang sering digunakan untuk layanan TI, sebesar 51%.

[7] 2023 North American Pulse of Internal Audit, The Institute of Internal Auditors, March 2023.

konsistensi yang lebih besar dalam upaya asurans teknologi dengan menentukan apakah fungsi manajemen risiko, kepatuhan, audit internal, dan fungsi lainnya memiliki sistem evaluasi dan pemeringkatan risikonya sendiri. Dalam diskusi dengan dewan dan manajemen, ketidakkonsistenan antar fungsi ini mungkin memberikan gambaran yang membingungkan atau mungkin tampak tidak lengkap. Audit internal dapat merekomendasikan dan memimpin upaya terkoordinasi dengan menggunakan taksonomi risiko yang umum. Komunikasi mengenai risiko kepada dewan dan manajemen senior akan lebih mudah dipahami jika fungsi audit internal dan lini kedua menggunakan bahasa yang sama. Hasil atau penilaian dari semua fungsi ini tidak harus sama, namun istilah dan pendekatan yang digunakan harus konsisten.

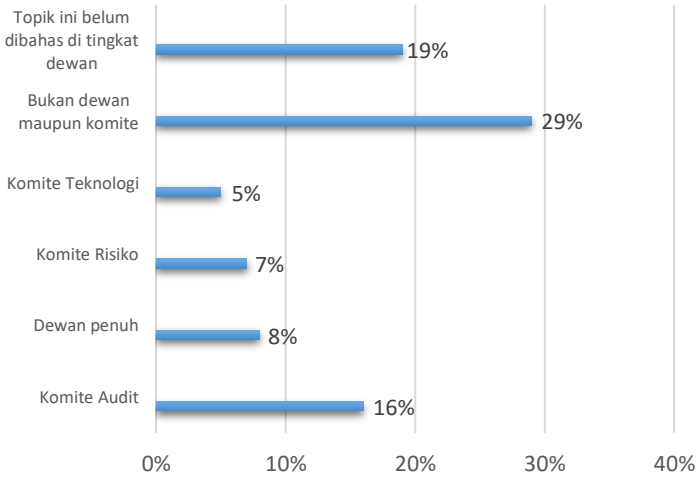
Mengawasi AI

Dengan banyaknya perusahaan yang masih bergulat dengan penggunaan AI dan AI generatif, auditor internal memiliki peluang untuk mendorong pengawasan yang lebih baik terhadap teknologi baru dan penggunaan teknologi tersebut oleh organisasi mereka.

Dalam survei[8] yang dilakukan Deloitte dan Society for Corporate Governance terhadap perusahaan-perusahaan besar dan menengah pada tahun 2023, hanya 13% yang memiliki kerangka pengawasan AI yang formal. Hanya 9% yang telah merevisi kebijakan perusahaan terkait keamanan siber, manajemen risiko, penyimpanan catatan, dan lainnya untuk mengatasi penggunaan AI. Namun, *National Association of Corporate Directors* mencatat bahwa tahun sebelumnya, 94% responden perusahaan mengatakan bahwa AI sangat penting bagi kesuksesan jangka pendek perusahaan mereka.[9]

Meskipun pentingnya AI, dewan tampaknya belum mengatasi permasalahan terkait. Survei tersebut menemukan bahwa total 48% dewan responden belum mempertimbangkan AI atau belum menetapkan tanggung jawab untuk hal tersebut (lihat grafik). Di antara mereka yang telah menugaskan tanggung jawab untuk AI, kemungkinan besar mereka berada di bawah pengawasan komite audit, yang sering kali merupakan kelompok yang berada di bawah tanggung jawab *chief audit executive* mereka. Audit internal dapat memberikan nilai tambah yang besar dengan membantu organisasi mengenali dan mengatasi kesenjangan antara pentingnya AI dan respons mereka terhadap AI.

Siapa yang memiliki pengawasan utama terhadap AI di Dewan?



Sumber: *Deloitte and Society for Corporate Governance Board Practices Quarterly: Future of tech: Artificial intelligence (AI)*, Agustus 2023.
Catatan: Respons "Lainnya/tidak tahu" tidak termasuk dalam grafik.

[8] *"Deloitte and Society for Corporate Governance Board Practices Quarterly: Future of tech: Artificial intelligence (AI),"* August 2023.
[9] "Artificial Intelligence: An Emerging Oversight Responsibility for Audit Committees?" Brian Cassidy, Ryan Hittner, and Krista Parsons, NACD 2024 Governance Outlook.

Simpulan

Asurans teknologi yang mengidentifikasi risiko dan hambatan sudah terintegrasi dengan baik ke dalam peran audit internal. Sambil mempertahankan fokus pada beberapa kerentanan terbesar yang berhubungan dengan teknologi, audit internal juga dapat mendorong peningkatan koordinasi upaya untuk memastikan gambaran yang lebih lengkap dan akurat bagi manajer risiko dan pemangku kepentingan. Langkah-langkah yang diuraikan dalam laporan singkat ini dapat membantu memastikan bahwa pendekatan organisasi secara keseluruhan terhadap risiko teknologi dan rencana audit cukup mengatasi potensi risiko teknologi.

Bagian 2: Tetap Mengikuti Perkembangan Adopsi Teknologi Organisasi

Tentang Ahli

Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, adalah manajer produk di TeamMate Audit Solutions, dimana dia bekerja untuk terus meningkatkan produktivitas audit sambil memberikan wawasan strategis melalui solusi TeamMate yang terbaik di kelasnya. Beliau memiliki lebih dari 20 tahun pengalaman audit internal baik di sektor publik maupun swasta.

Sebelumnya, Jim memegang sejumlah peran kepemimpinan di The Institute of Internal Auditors, menjabat sebagai Auditor Pemerintah Kota untuk Kota Palo Alto, CA, dan Kepala Audit untuk Wilayah San Diego, CA. Latar belakang audit internalnya yang beragam mencakup posisi di California State University System, PETCO Animal Supplies, Inc., State Street Corporation, dan General Electric.

Dennis Wong, CIA, CFSA

Dennis Wong, CIA, CFSA, adalah direktur pelaksana di sebuah bank internasional yang berbasis di London. Beliau adalah seorang profesional berpengalaman di bidang audit dan risiko, dengan pengalaman lebih dari 20 tahun di perbankan internasional dan pasar modal. Semangatnya adalah memimpin dan mendorong perubahan melalui rekayasa ulang proses dan inovasi teknologi. Dia menjadi sukarelawan di IIA Cabang New York dan bertugas di Komite Pengembangan Ujian global.

Pendahuluan

Teknologi telah menjadi sumber kehidupan organisasi, alat vital yang digunakan secara teratur di setiap fungsi. Namun meskipun 60% pemimpin bisnis dan risiko melihat satu alat teknologi baru, AI generatif (GenAI), sebagai sebuah peluang, 57% mengatakan bahwa persiapan investasi dalam teknologi baru adalah pemicu terbesar untuk meninjau lanskap risiko, menurut PwC Survei Risiko Global 2023. [10]

Teknologi menawarkan manfaat baru, namun ketergantungan terhadap teknologi juga membawa ancaman, ancaman yang semakin besar seiring dengan semakin kritis dan meluasnya penggunaan teknologi. Hal ini mencakup risiko yang terkait dengan cara adopsi teknologi. Audit internal dapat membantu organisasi menentukan dan melaksanakan strategi penerapan terbaik untuk meminimalkan risiko dan meningkatkan nilai teknologi baru. Laporan singkat ini membahas langkah-langkah yang dapat diambil audit internal untuk memberikan nilai tambah dalam upaya ini.

[10] "Cyber and Digital Technology Risks Are a Key Concern for Businesses and Risk Leaders, Even as 60% See GenAI as an Opportunity: PwC 2023 Global Risk Survey," PwC press release, November 20, 2023.

Mengembangkan Kerangka Tata Kelola Baru

Bagaimana teknologi baru bisa diterapkan?

Audit internal dapat membantu memandu adopsi teknologi

Teknologi baru selalu menghadirkan pertimbangan risiko baru. Meskipun GenAI, misalnya, telah menginspirasi banyak penggunaan inovatif untuk teknologi transformatif ini, GenAI juga menghadirkan bahaya baru di bidang-bidang yang mencakup privasi, bias yang melekat, serta transparansi dan keakuratan informasi yang diterima. Pada saat yang sama, risiko dapat muncul ketika teknologi baru mendorong perubahan dalam operasi bisnis, yang memapar risiko operasional baru bagi organisasi.

Oleh karena itu, ketika mengadopsi teknologi baru, organisasi harus mengembangkan kerangka tata kelola proyek yang kuat yang mempertimbangkan bagaimana alat baru tersebut cocok dengan bisnis, menyelaraskan dengan strategi perusahaan, dan membantu mencapai tujuan perusahaan, kata Dennis Wong, CIA, CFSA, seorang professional audit dan risiko yang berpengalaman, dengan pengalaman lebih dari 20 tahun di perbankan internasional dan pasar modal. Memang benar, di antara perusahaan-perusahaan yang ditetapkan sebagai "pelopor risiko" dalam survei PwC, 73% cenderung memiliki strategi dan peta jalan teknologi di seluruh perusahaan, dibandingkan dengan 57% organisasi yang kurang maju. Kerangka kerja tersebut harus mencakup pertimbangan risiko yang luas, termasuk penilaian risiko komprehensif dan pengendalian yang dapat mengatasi ancaman yang ditimbulkan oleh risiko baru, kata Wong.

Audit internal dapat memberikan jaminan atas tata kelola proyek dan seberapa baik kinerjanya, serta dapat memberikan saran mengenai adopsi teknologi secara umum. Pada awalnya, audit internal dapat melakukan tinjauan pra-implementasi yang mempertimbangkan kesesuaian teknologi serta risiko terkait dan perubahan pengendalian yang diperlukan. Ketika alat-alat baru sudah ada, audit internal juga dapat memberikan umpan balik tentang cara kerja penerapan teknologi dan dampak alat-alat baru tersebut terhadap seluruh organisasi, menurut Wong. Setelah penerapannya, audit internal dapat mempertimbangkan apakah teknologi tersebut berfungsi sebagaimana yang diharapkan, dan apabila tidak, diberikan penjelasan mengenai penyebabnya, termasuk apakah manfaat yang diharapkan telah tercapai.

Audit internal juga dapat menemukan hambatan yang mungkin mengganggu penerapannya. Perusahaan yang sangat terkotak-kotak mungkin akan mengalami pemikiran *silo*, yang mana para profesional di berbagai fungsi tidak menyadari apa yang terjadi di bidang lain. Suatu area mungkin tidak mengetahui bahwa kelompok lain sedang mengeksplorasi teknologi yang sama namun telah menemukan kegunaan yang berbeda, atau bahwa fungsi ketiga telah menghadapi beberapa kegagalan dengan teknologi tersebut namun mendapatkan pelajaran yang berharga. "Hal ini dapat menciptakan perpecahan ketika Anda mencari sinergi," menurut Wong. Karena audit internal memiliki pandangan holistik terhadap organisasi, maka audit internal mempunyai posisi yang unik untuk menghilangkan *silo-silo* ini dan menawarkan wawasan menyeluruh yang mencegah duplikasi upaya. "Karena pengetahuan institusionalnya, audit internal dapat membawa perspektif baru yang dapat mengarah pada penggunaan teknologi yang lebih bernilai," ujarnya. Hal ini juga dapat memberikan jaminan apakah pengendalian operasional berfungsi dengan baik dan memastikan penggunaan teknologi aman dan terjamin. Karena dana investasi selalu terbatas, organisasi akan menghargai saran mengenai apakah pengeluaran teknologi mereka dimanfaatkan sebaik-baiknya, kata Wong.

Organisasi perlu mengatasi keterkaitan antara risiko strategis dan operasional serta teknologi yang mendasarinya. "Yang satu berdampak pada yang lain," kata Wong. Teknologi baru mengubah cara organisasi beroperasi, sehingga membawa risiko baru. Hal ini pada gilirannya dapat mendorong perubahan dalam operasional yang dapat menimbulkan risiko tambahan. Kuncinya adalah memiliki pemahaman yang jelas mengenai tujuan organisasi, bagaimana tujuan tersebut dipengaruhi atau membawa risiko baru, dan pengendalian apa yang dapat mengatasi permasalahan ini.

Organisasi juga akan mendapatkan manfaat dari budaya risiko yang kuat, mengingat perubahan yang ditimbulkan oleh teknologi baru. Bahkan jika organisasi memiliki pola pikir pengendalian dan kerangka pengendalian yang kuat, organisasi tersebut masih perlu bergantung pada individu untuk menerapkan pengendalian atau mengambil langkah yang tepat saat mereka tidak ada, kata Wong, sehingga disiplin risiko yang kuat dan pemahaman yang tepat mengenai risiko teknologi baru sangatlah penting. Budaya perusahaan harus mengidentifikasi dan mengkomunikasikan potensi ancaman dari alat-alat baru dan ekspektasi perusahaan dalam penggunaannya sehingga dapat dipahami oleh semua orang.

Mempertimbangkan Langkah yang Terukur

Menemukan keseimbangan antara kecepatan dan keamanan

Memberi advis tentang kapan harus menggunakan teknologi baru

Seringkali terdapat keadaan mendesak untuk menerapkan teknologi baru ketika teknologi baru telah diperkenalkan, dalam kondisi belakangan ini digambarkan dengan terburu-buru menerapkan GenAI. Karena potensi risiko yang terkait dengan alat-alat baru, "organisasi perlu menemukan keseimbangan yang tepat antara kecepatan dan keselamatan," kata Wong. Dia menunjuk pada mobil, yang tidak memiliki sabuk pengaman saat pertama kali diperkenalkan, namun menambahkan lebih banyak fitur keselamatan selama bertahun-tahun seiring mobil mulai bergerak lebih cepat. Mengingat tingkat perubahan teknologi saat ini dan kompleksitas sistem yang terlibat, audit internal dapat membantu memeriksa apakah manajemen telah menerapkan fitur – atau pengendalian keselamatan yang tepat. "Risikonya, baik teridentifikasi atau tidak, dimulai sejak hari pertama," kata Wong. "Hal ini mungkin tidak langsung menjadi kerugian atau ancaman, namun begitu Anda mulai menggunakan suatu teknologi, Anda sudah dihadapkan pada risiko tersebut."

Sebagai contoh, GenAI adalah alat canggih dengan kompleksitas berlapis; mudah bagi pelaku kejahatan untuk mengeksploitasinya untuk tujuan jahat. Selain itu, staf yang belum terlatih dengan baik mengenai risiko GenAI mungkin tanpa disadari memasukkan data rahasia atau sensitif, yang dapat dimasukkan ke dalam pelatihan program dan dapat diakses oleh pihak luar.

Organisasi harus mempertimbangkan apakah akan menjadi yang pertama memasarkan dan menghadapi risiko dari sumber yang tidak terduga dan potensi kerusakan bisnis atau reputasi, atau apakah mereka harus mengadopsi strategi pengikut cepat (*quick follower*) untuk belajar dari pengalaman dan kesalahan pihak lain.

Memahami Utang Teknis (*Technical Debt)*

Infrastruktur, staf, budaya mungkin tidak dapat menangani teknologi terbaru

Mengidentifikasi *technical debt* dan langkah-langkah perbaikannya

Organisasi juga perlu menentukan apakah infrastruktur mereka yang ada saat ini dapat menangani alat teknologi baru. Ketika teknologi diadopsi, tekanan waktu, pertimbangan biaya, atau hambatan lain sering memaksa organisasi untuk mengambil jalan pintas untuk memenuhi tenggat waktu, atau terdapat juga tantangan lain yang dapat menyebabkan organisasi gagal mencapai implementasi yang optimal. *Technical debt* ini dapat menumpuk dari waktu ke waktu jika organisasi gagal meningkatkan ke versi perangkat lunak baru atau perangkat keras baru, untuk mengimplementasikan *patches*, atau untuk mengambil langkah-langkah pemeliharaan utama lainnya, kata Jim Pelletier, CIA, CGAP, manajer senior produk dengan TeamMate Audit Solutions. Karena organisasi terus-menerus mengadopsi solusi baru untuk menjaga sistem tetap berjalan, kelincahan teknisnya semakin tertinggal.

Technical debt dapat mencegah organisasi memanfaatkan perangkat lunak yang ada dengan sebaik-baiknya atau bahkan membuat tidak mungkin untuk mengadopsi teknologi baru secara efektif, kata Pelletier. Masalahnya mungkin tidak dikomunikasikan dengan baik oleh tim TI karena mereka tidak menyadarinya, enggan membahas kegagalan sistem, atau menganggap teknologi terlalu rumit untuk dijelaskan kepada profesional non-teknologi. Akibatnya, auditor internal mungkin tidak menyadari *technical debt* ini atau dampaknya terhadap kemampuan organisasi untuk mengadopsi teknologi baru.

Pertanyaan untuk Ditanyakan tentang Teknologi Baru

Dalam memberikan asurans atau advis, beberapa pertanyaan yang dapat diajukan oleh audit internal meliputi:

- Apa dampak teknologi baru terhadap organisasi dan proses bisnisnya, termasuk risiko, manfaat, dan peluang baru?
- Bagaimana teknologi sesuai dengan manajemen risiko perusahaan dan pendekatan tata kelola, risiko, dan kepatuhan organisasi?
- Bagaimana seharusnya teknologi diintegrasikan dengan pengendalian yang ada? Apakah sudah ada evaluasi dampak terhadap pengendalian internal? Jika demikian, perubahan apa yang harus dilakukan dalam pengendalian dan proses? Haruskah audit internal bekerja dengan masing-masing unit bisnis untuk mengevaluasi kembali risiko dan pengendalian mereka dan bersiap untuk mendokumentasikan risiko dan pengendalian baru?
- Apakah kita perlu melakukan peningkatan teknologi, perubahan proses bisnis, atau peningkatan keterampilan karyawan kita?
- Risiko baru apa yang diperkenalkannya, termasuk ancaman terhadap privasi, data pelanggan, informasi kepemilikan, dan lainnya?
- Di mana sistem baru digunakan dan oleh siapa?
- Apa yang terjadi pada data yang dikumpulkan atau diproduksi oleh teknologi tersebut? Di mana data tersebut disimpan dan bagaimana data dilindungi?
- Apakah organisasi sekarang berbagi data yang seharusnya tidak atau mengekspos organisasi pada risiko privasi data yang baru?

Meskipun audit internal tidak memerlukan keahlian yang sama dengan tim teknologi organisasi, audit internal dapat mengatasi masalah *technical debt* dengan mengambil langkah-langkah untuk memastikan orang-orangnya mempertahankan keterampilan yang cukup untuk melakukan dialog produktif dengan tim TI yang dapat mengungkapkan keadaan sistem organisasi saat ini, kata Pelletier. Berbekal pengetahuan ini, anggota tim audit internal dapat melakukan percakapan bermanfaat yang menghormati waktu dan keahlian anggota tim TI.

Dalam kasus lain, bahkan jika infrastruktur teknologi organisasi memadai, teknologi dapat berjalan maju dari perusahaan dan orang-orangnya. Itu bisa terjadi ketika organisasi memodernisasi teknologi mereka tanpa membawa tenaga kerja atau proses bisnis mereka ke kondisi terbaru. Perusahaan mungkin menerapkan teknologi untuk meningkatkan efisiensi, tetapi gagal meluangkan waktu untuk menyelaraskan dan memahami bagaimana proses akan terpengaruh atau perlu diubah. "Orang-orang tidak tahu cara menggunakannya, yang membuang-buang waktu, energi, dan uang," kata Pelletier. "Ada kesempatan yang terlewatkan untuk melakukan perbaikan yang signifikan." Sekali lagi, audit internal memiliki pengetahuan kelembagaan yang diperlukan untuk mengajukan pertanyaan yang tepat untuk memastikan bahwa teknologi dan tujuan serta aset bisnis sama-sama sesuai.

Akhirnya, seiring dengan teknologi yang berkembang pesat, mudah untuk melupakan nilai sentuhan manusia, tetapi reviu dan penilaian manusia akan tetap penting untuk proses tersebut, menurut Wong. Alat seperti GenAI tidak hanya terkadang membuat kesalahan atau mengada-ada, jika digunakan dalam interaksi pelanggan atau manusia lainnya, alat ini mungkin melewatkan sinyal yang dapat dipahami manusia atau memberikan jawaban yang tidak dapat dijalankan sebagaimana yang umumnya diketahui oleh manusia yang akrab dengan pelanggan dan umumnya mengetahui hal tersebut tidak layak.

Mengatasi Beberapa Keterbatasan GenAI

GenAI disambut dengan antusiasme yang liar/membara ketika pertama kali diperkenalkan, tetapi kekurangannya, seperti yang dibahas dalam laporan ini, telah menimbulkan kekhawatiran. Ini bisa menjadi alat yang berharga dalam menangani adopsi teknologi dalam suatu organisasi, jika digunakan dengan benar. Jim Pelletier mengidentifikasi dua opsi untuk auditor internal yang ingin meningkatkan penggunaan GenAI mereka.

- Dalam beberapa kasus, GenAI membuat jawaban, atau berhalusinasi, jika tidak dapat menjawab pertanyaan, atau membuat kesalahan karena hanya tahu apa yang telah dilatih. Untuk mengatasi masalah itu, *Retrieval-Augmented Generation* (RAG) adalah teknik yang menyediakan data yang akurat dan tepat waktu untuk menambah apa yang ada dalam sistem GenAI. RAG mengoptimalkan model keluaran bahasa yang besar, seperti GenAI, dengan merujuk basis pengetahuan otoritatif di luar sumber data pelatihan GenAI sebelum respons dihasilkan. Dan sementara sumber GenAI belum transparan, RAG memungkinkan untuk mengidentifikasi sumber bahannya.
- Mendapatkan output terbaik dari GenAI sebagian bergantung pada pemberian arah/instruksi yang benar, yang dikenal sebagai petunjuk *(prompt)*. *Prompt* harus menentukan detail seperti berapa lama respons seharusnya, audiens untuk respons tersebut jika akan dibagikan dengan orang lain, gaya, dan juga nadanya. Pelletier memberikan contoh:

  Anda adalah manajer audit internal berpengalaman dengan keahlian dalam manajemen risiko teknologi di industri jasa keuangan. Anda mengevaluasi risiko teknologi berdasarkan dampak terhadap operasi bisnis dan kemungkinan risiko akan terjadi.

  - Dalam format tabel, identifikasi 10 risiko teratas yang terkait dengan adopsi teknologi baru di bank besar.
  - Sertakan kolom untuk Nama Risiko, Deskripsi Risiko, dan Alasan, yang menjelaskan mengapa risiko menjadi prioritas utama.
  - Prioritaskan baris tabel dari risiko tinggi ke risiko rendah.

Kesimpulan

Meskipun menerapkan teknologi baru dapat membawa risiko, penting juga untuk mengingat bahaya dari gagalnya mengikuti perkembangan terkini dari alat-alat baru. Banyak kelemahan dari melakukannya termasuk :

- Kehilangan manfaat yang dapat ditawarkan teknologi baru.
- Gagal bersaing dengan pesaing karena keuntungan yang mereka peroleh dari transformasi digital.
- Kehilangan peningkatan efisiensi dan produktivitas atau gagal berinovasi pada produk dan layanan baru.
- Kehilangan pelanggan potensial atau pelanggan yang sudah ada, mitra bisnis yang berharga, atau karyawan berbakat yang lebih suka bekerja dengan organisasi yang lebih maju secara teknologi.

"Teknologi mendasari semua yang kita lakukan setiap hari," kata Pelletier. Audit internal dapat berperan dalam memastikan bahwa alat baru memiliki dampak positif secara maksimum.

Part 3: Tantangan Mengenai Talenta Teknologi Audit Internal

Tentang Para Ahli

Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, adalah seorang *senior product manager* di TeamMate Audit Solutions, di mana dia bekerja untuk terus meningkatkan produktivitas audit sambil memberikan wawasan strategis melalui solusi TeamMate yang terbaik di kelasnya. Dia memiliki lebih dari 20 tahun pengalaman audit internal baik di sektor publik maupun swasta.

Sebelumnya, Jim memegang sejumlah peran kepemimpinan di The Institute of Internal Auditors, menjabat sebagai Auditor untuk Kota Palo Alto, CA, dan Kepala Audit untuk Wilayah San Diego, CA. Latar belakang audit internalnya yang beragam mencakup posisi di California State University System, PETCO Animal Supplies, Inc., State Street Corporation, dan General Electric.

Dennis Wong, CIA, CFSA

Dennis Wong, CIA, CFSA, adalah direktur pelaksana di sebuah bank internasional yang berbasis di London. Dia adalah seorang profesional audit dan risiko dengan pengalaman lebih dari 20 tahun di perbankan internasional dan pasar modal. Semangatnya adalah memimpin dan mendorong perubahan melalui rekayasa ulang proses dan inovasi teknologi. Dia menjadi sukarelawan di IIA Cabang New York dan bertugas di Komite Pengembangan Ujian global.

Nisha Nair, CIA, FCCA, UAECA, CFE, ACMA, CGMA

Nisha Nair bekerja sebagai spesialis audit internal di Otoritas Federal untuk Regulasi Nuklir di Uni Emirat Arab. Dia telah memiliki lebih dari 10 tahun pengalaman sebagai profesional penasihat risiko keuangan dan bisnis, termasuk bekerja di konsultan risiko di perusahaan konsultan 'Big 4'. Dia adalah anggota dari berbagai badan kualifikasi profesional dan mempromosikan nilai profesi audit internal. Selain itu, beliau menjabat sebagai ahli di bidang Global Professional Knowledge Group untuk IIA Global, dengan keahlian yang mencakup berbagai bidang terkait audit internal termasuk manajemen risiko, analisis data, tata kelola, manajemen risiko penipuan, etika, dan audit eksternal.

Pendahuluan

Celah dalam pertahanan audit internal

Menurut 2024 North American Pulse of Internal Audit, keamanan siber dan TI dipilih oleh para pemimpin audit internal sebagai dua bidang dengan risiko tertinggi di organisasi mereka, dengan 78% dan 58% responden masing-masing menilai bidang tersebut sebagai risiko tinggi atau sangat tinggi. Hal ini seharusnya tidak mengejutkan; memang, teknologi telah mendominasi lanskap risiko selama beberapa tahun terakhir. Namun, dari tahun ke tahun semakin jelas bahwa audit internal menghadapi tantangan serius dalam bidang ini yang akan menjadi lebih buruk jika tidak diatasi.

Gabungan upaya keamanan siber dan TI mencakup hampir 20% rencana audit, menurut responden survei Pulse, yang sebagian besar merupakan pemimpin audit di Amerika Utara. Kedua hal ini merupakan area risiko tertinggi dibandingkan area risiko lainnya, namun Pulse juga menunjukkan bahwa keamanan siber dan data serta TI merupakan area yang paling banyak di-*outsource* atau *co-source*. Selain itu, meskipun sekitar 2 dari 10 responden menyatakan bahwa teknologi akan menjadi prioritas utama, hampir separuh fungsi audit memprioritaskan penambahan staf internal. Hal ini terjadi meskipun fungsi audit terus menghadapi berbagai masalah dalam perekrutan, dengan 29% responden Pulse menyebut ekspektasi kompensasi sebagai tantangan paling signifikan, diikuti oleh 17% yang mengatakan calon karyawan kurang memiliki kompetensi yang dibutuhkan.

Secara keseluruhan, fakta-fakta ini memberikan gambaran yang menunjukkan bahwa meskipun audit internal bisa mendapatkan kemampuan dalam risiko teknologi melalui *outsourcing* dan *co-sourcing*, hal ini bukanlah cara yang ideal dalam membawa kompetensi ini ke dalam organisasi. Dalam jangka panjang, cara ini dapat menimbulkan dampak yang signifikan tidak hanya pada cakupan risiko, namun juga pada kemampuan fungsi audit dalam memanfaatkan teknologi guna meningkatkan peran mereka.

Sebagai bagian terakhir dari tiga bagian dalam inovasi dan teknologi yang disponsori oleh TeamMate, pengetahuan ini mengkaji secara ringkas sejumlah aspek dari apa yang disebut sebagai “tantangan teknologi” audit internal, misalnya usaha untuk membangun tim yang paham teknologi (*tech-savvy*). Dengan masukan dari pakar industri, hal ini juga akan memberikan beberapa praktik terbaik dan strategi terlepas dari ukuran industri, anggaran, atau fungsi yang dapat digunakan untuk memberikan layanan asurans dan advisori yang dapat mengimbangi perkembangan teknologi yang semakin cepat dan tiada henti.

Membangun Tim Teknologi

Bersiap Saat Ini untuk Masa Depan Teknologi

Masalah pendanaan

Audit internal tidak sendirian dalam usaha untuk memperoleh talenta yang melek teknologi. Faktanya, hampir semua departemen di setiap organisasi di setiap industri mengalami tantangan yang sama, sehingga menciptakan persaingan yang ketat untuk merekrut dari sekelompok talenta yang sebelumnya jumlahnya terbatas. Menyusul PHK masal di sektor teknologi selama pandemi COVID-19, banyak analis memperkirakan sekitar 20.000 pekerja industri teknologi akan mencari pekerjaan untuk memenuhi kebutuhan ini. Namun, sebagai bukti pesatnya evolusi teknologi, kesenjangan antara posisi yang dibutuhkan dan talenta yang cukup terampil semakin melebar – dan talenta yang tersedia untuk dipekerjakan tidaklah murah. Dengan melihat data Pulse, bahwa 51% fungsi audit memiliki anggaran yang sama dari tahun sebelumnya, jelas bahwa setiap fungsi audit yang ingin masuk ke dalam perekrutan talenta teknologi memiliki tantangan besar di depan mereka.

“Topik yang paling sering muncul ketika para pemimpin audit internal berbicara tentang kesulitan penerapan teknologi adalah tentang pentingnya pendanaan yang memadai,” kata Nisha Nair, spesialis audit internal pada Otoritas Federal untuk Regulasi Nuklir di Uni Emirat Arab. “Ini termasuk pendanaan untuk peralatan TI, pelatihan teknologi bagi staf audit internal, dan mempekerjakan sumber daya teknologi yang tepat dalam tim. Seringkali ketika mencoba merekrut seseorang spesialis dalam bidang tertentu seperti industry siber, ekspektasi mereka akan remunerasi akan jauh lebih tinggi dibandingkan audit internal pada umumnya, banyak dari mereka juga lebih memilih untuk bekerja dan berkembang di bidang khusus mereka dengan gaji lebih tinggi dibandingkan peran audit internal yang bersifat generalis.”

Dalam kenyataan yang sulit ini, bahkan hanya untuk mengimbangi risiko yang disebabkan teknologi, audit internal harus kreatif dalam mengisi *skill gap* yang ada. “Strategi dalam hal *skillset* ini tidak bersifat *one-size-fits-all*,” kata Dennis Wong, direktur pelaksana dan kepala audit risiko kejahatan keuangan global di HSBC. “Kombinasi yang tepat akan berbeda pada setiap unit audit. Hal ini merupakan kombinasi dari pengembangan/peningkatan keterampilan secara organik, kerja sama dengan konsultan, dan perekrutan eksternal.”

Setiap elemen dari strategi tiga aspek ini layak untuk didiskusikan:

Perekrutan Eksternal

Seperti disebutkan sebelumnya terkait kondisi anggaran saat ini dan kurangnya pendanaan tambahan, penerapan strategi ini mungkin terlihat sebagai pemikiran yang tidak realistis dan bahkan diabaikan sama sekali. Namun, meskipun hal ini disebut tantangan, pertimbangan terkait perekrutan eksternal mungkin terjadi – dan hal ini dimulai dari komite audit

Karena Dewan dan/atau Komite Audit mempunyai peran kuat dalam persetujuan anggaran audit, tujuan pemimpin audit adalah membuat alasan kuat terkait perlunya tambahan dana untuk perekrutan staf teknis dalam rangka penerapan teknologi dan inovasi. Hal ini lebih dari sekedar mengutip data; sebaliknya, tujuannya adalah “menyampaikan cerita yang menarik” yang sulit ditolak, kata Nair. “Para pemimpin audit harus mendapatkan dukungan dari Komite Audit dan Manajemen Senior mengenai kebutuhan talenta teknologi di departemen audit, nilai yang harus diberikan kepada organisasi, dan menjelaskan perlunya paket remunerasi dan jalur karier yang tepat untuk menarik talenta tersebut masuk di departemen audit,” kata Nair.

“Kita harus mendapatkan dukungan komite audit dan menyadarkan mereka bahwa talenta ini adalah talenta yang khusus, dan bahwa paket remunerasi yang berlaku untuk tim audit mungkin tidak cukup untuk seseorang yang berkecimpung di bidang siber,” katanya.

Hal ini mungkin akan mengharuskan komite audit untuk mempertimbangkan kembali seberapa efektif struktur tim audit internal untuk lingkungan risiko saat ini. Apa yang dibutuhkan staf audit saat ini sangat berbeda dibandingkan 15 tahun yang lalu. “Melihat gambaran besarnya, kita perlu memikirkan seperti apa tim yang kita inginkan nanti,” kata Jim Pelletier, manajer produk senior di TeamMate Audit Solutions. “Saat ini, Anda tidak mempekerjakan auditor tradisional, Anda merekrut pakar keamanan siber – itulah peran yang perlu Anda miliki. Pemimpin audit perlu menjelaskan kepada komite bahwa mereka tidak dapat menawarkan tarif auditor internal, karena mereka tidak mempekerjakan auditor internal. Mereka bahkan mungkin tidak memakai istilah 'audit' pada nama jabatanya.”

Sebagai salah satu upaya, pakar keamanan siber tidak harus tersedia secara eksplisit di audit internal. “Mereka dapat dipakai ketika keahlian mereka diperlukan saja,” kata Pelletier. “Saat saya melakukan audit keamanan siber, saya akan melakukannya secara komprehensif, namun pelaksanaannya tidak perlu terus-menerus, jadi saya hanya memerlukan keterampilan tersebut mungkin hanya beberapa kali dalam setahun. Sudah saatnya audit internal menjadi kreatif. Saya tidak perlu membawa spesialis siber ke dalam tim saya setiap saat, namun saya dapat menggunakan spesialis siber yang biasanya bekerja di lini kedua sebagai auditor bila diperlukan, hal ini akan sangat efektif dan efisien selama saya tetap memperhatikan independensi dan objektivitas.”

Topik ini tidak boleh berakhir di Komite Audit atau Dewan Direksi, melainkan pemimpin audit internal harus menggunakan posisinya sebagai *advisor* untuk mengomunikasikan nilai dari talenta teknologi yang terampil. “Para pemimpin audit dapat menjadi pembawa perubahan,” lanjut Nair. “Mereka perlu memiliki komunikasi yang berorientasi pada teknologi dengan manajemen dan memberi navigasi kepada organisasi menuju masa depan yang lebih mendukung teknologi.” Dengan komunikasi seperti itu di tingkat atas, akan menyebar ke departemen lain dalam organisasi. Hal ini membantu menciptakan lingkungan kolaboratif untuk mengembangkan atau memungkinkan solusi teknologi mencapai tujuan bersama. Dengan dukungan organisasi yang cukup, pendanaan pasti akan mengikuti.

Hal yang juga penting dalam pencarian talenta adalah memanfaatkan setiap cara dalam memperluas kelompok. Hal ini dapat dicapai dengan berbagai cara. Misalnya, fokus pada inisiatif *diversity, equity,* dan *inclusion (DEI)* tidak hanya mendorong kecerdasan kognitif dalam organisasi namun juga membuat organisasi lebih menarik bagi generasi muda yang terampil. Selain itu, departemen yang membuka posisi kosong harus mempertimbangkan dengan matang untuk memperluas kelompok dengan menyertakan opsi kerja jarak jauh. Menurut Pulse, secara mengejutkan, 95% pemimpin audit generasi Milenial (1981-1996) memperkirakan tingkat kerja jarak jauh akan tetap sama, yang berarti ada ekspektasi bahwa karyawan di masa depan akan mencari opsi semacam itu.

Terakhir, dalam perekrutan, sadarilah bahwa teknologi berkembang begitu cepat sehingga banyak kompetensi yang mungkin ada dalam deskripsi pekerjaan menjadi ketinggalan jaman dalam hitungan tahun atau bulan. Oleh karena itu, manajer perekrutan tidak boleh terlalu kaku dalam memeriksa keterampilan bagi para kandidat. Kuncinya bukanlah seberapa baik seseorang mengetahui teknologi tertentu, melainkan kemampuan mereka untuk terus mengembangkan diri. “Kami tidak menyarankan Anda mempekerjakan seseorang untuk teknologi tertentu, melainkan seseorang yang dapat memahami teknologi baru dengan mudah,” kata Nair. “Fungsi audit membutuhkan orang-orang yang mudah beradaptasi, dalam hal mampu menyerap keterampilan baru seperti sebuah spons.”

Tipe individu inilah yang akan mendapat manfaat terbesar dari kerja sama dalam tim yang menempatkan mereka pada posisi untuk belajar dan sukses. “Sangat jarang menemukan *unicorn* individu yang 'tunggal' memiliki semua keterampilan risiko, pengetahuan bisnis, audit, serta ilmu data dan teknologi. Hal ini bukan tidak mungkin, namun jarang terjadi,” kata Wong. “Jadi, prioritasnya haruslah pada pembentukan tim yang terdiri dari orang-orang yang bekerja sama secara kolektif, seperti ilmuwan data yang bekerja sama dengan auditor internal yang dapat belajar dan berkembang melalui proses audit.”

Outsourcing **dan** ***Co-Sourcing*** **dalam Peningkatan Keterampilan**

Seperti disebutkan sebelumnya, banyak fungsi audit saat ini memilih untuk melakukan *outsourcing* dan *co-source* tanggung jawab audit siber dan TI mereka. Tren ini jelas berasal dari kebutuhan mengingat tantangan dan kendala perekrutan, namun khususnya di bidang teknologi seperti keamanan siber, hal ini juga merupakan suatu kebutuhan.

“Secara internal, sangat sulit mendapatkan pengetahuan tentang teknologi terkini dan terbaik,” kata Wong. “Anda harus melihat keluar perusahaan Anda untuk mencari keahlian itu. Di sinilah konsultan dan spesialis berperan.”

Namun, ketika mendatangkan firma-firma luar ini, kadang-kadang diabaikan tentang bagaimana talenta yang dialihdayakan dapat berdampak pada fungsi audit melebihi jangka waktu kontrak mereka.

“Yang berhasil dengan baik adalah ketika Departemen Audit memanfaatkan pemasok Audit, mitra Audit, dan/atau konsultan yang ada untuk meningkatkan keterampilan staf IA di departemen mereka sendiri, sementara talenta yang di-*outsourced/co-source* melaksanakan pekerjaan audit tertentu,” kata Nair. “Ada baiknya untuk memasangkan talenta/mitra/konsultan *outsourcing/co-sourced* dengan staf audit untuk memungkinkan transfer pengetahuan saat keterlibatan sedang dilaksanakan. Pembelajaran di tempat kerja terbukti lebih efektif.”

Pelletier setuju.

"Jika kita melakukan alih daya atau *co-sourcing*, tidak apa-apa, tetapi apakah Anda membaik?" dia bertanya. "Apakah Anda menanamkan staf Anda ke dalam proyek mereka sehingga mereka belajar? Apakah Anda memanfaatkan sepenuhnya waktu yang Anda miliki untuk membangun lebih banyak keahlian internal?"

Hal ini juga merupakan ide yang bermanfaat untuk menyebarkan kompetensi teknologi dasar dari talenta *outsourcing* dan *co-sourcing* dengan cara yang lebih terstruktur. Hal ini dapat berupa lokakarya atau sesi kelompok dimana individu dari semua departemen dapat melihat secara langsung kemungkinan-kemungkinan teknologi, dan kemudian mereka dapat membawa pengetahuan yang baru, kembali ke bidangnya masing-masing.

Namun, setelah keterampilan tim ditingkatkan atau keahlian tim direkrut secara penuh, *co-sourcing* harus selalu menjadi bagian dari strategi keahlian organisasi. "Setelah telenta berketerampilan tinggi diangkat sebagai karyawan penuh waktu, mereka pasti akan kehilangan keunggulannya," kata Wong. "Dalam keamanan siber, misalnya, jika Anda membawa peretas topi putih dengan keahlian teknologi terkini untuk melakukan hal-hal, seperti uji penetrasi. Tetapi jika mereka tidak lagi 'meretas', mereka tidak akan lagi menjadi yang terdepan dalam bidang tersebut. Jadi, terlepas dari tingkat keahlian tim internal, Anda akan selalu ingin menyewa perusahaan luar sampai batas tertentu karena mereka akan selalu mengetahui kerentanan terkini.”

Peningkatan Keterampilan Dari Dalam ke Luar

Meskipun sebagian besar diskusi mengenai teknologi berkisar pada mendatangkan talenta, penting untuk tidak mengabaikan talenta yang sudah ada di dalam perusahaan. Melalui hubungan positif dan kolaborasi antara audit internal, manajemen senior, dan tim TI, audit internal harus bekerja untuk mengembangkan pemahaman yang jelas tentang keterampilan dan alat yang dimiliki departemen lain. Analisis data atau perangkat lunak untuk pemantauan berkelanjutan, misalnya, dapat memiliki aplikasi luas yang dapat disesuaikan dengan tugas audit dengan sedikit pelatihan.

“Anda harus bekerja sama dengan tim lain dan menjelajahi berbagai cara di mana Anda dapat berkolaborasi — dan jika hubungannya baik, mereka mungkin dapat mengatakan sesuatu seperti, 'Oke, kami sudah memiliki alat ini, jadi mengapa kami tidak menggunakannya untuk tujuan audit internal?'” kata Wong.

Ini juga berlaku untuk manajemen senior. Sebagai lini kedua, mereka mungkin memiliki akses ke alat analisis data, alat pemantauan dan audit berkelanjutan (*Continuous Audit and Continuous Monitoring* - CACM), dan alat yang berhubungan dengan ISO dan prosedur – yang semuanya dapat berguna dalam konteks audit internal.

Tentu saja, kebutuhan akan peningkatan keterampilan lebih dari sekedar audit internal saja. Yang pasti, dorongan untuk meningkatkan kompetensi teknologi dasar di seluruh organisasi harus ada di seluruh di lingkungan saat ini. Sekali lagi, dengan memanfaatkan peran mereka sebagai pembawa perubahan, para pimpinan audit internal harus melakukan advokasi di semua interaksi departemen mereka untuk pelatihan wajib mengenai tren dan teknik teknologi saat ini. “Pendekatan yang efektif adalah dengan menentukan tingkat minimum pengetahuan dan keterampilan terkait teknologi atau data serta tingkat kemajuan/keahlian untuk setiap posisi dalam kerangka kompetensi IA,” kata Nair. “Kita perlu mendorong setiap profesional IA untuk menjalani pelatihan minimum yang diperlukan untuk mempelajari setidaknya keterampilan TI dasar untuk posisi pekerjaan mereka dan kemajuannya.”

Wong mengungkapkan sentimen serupa. “Peningkatan keterampilan di semua peran selalu dibutuhkan,” katanya. “Menjaga relevansi dan mengimbangi pasar adalah suatu keharusan. Selalu ada alat dan teknik baru yang perlu diperhatikan.”

Mendapatkan keterampilan seperti itu tidak selalu harus melibatkan peningkatan anggaran pelatihan. Banyak dari keterampilan ini dapat dipelajari baik secara individu melalui kursus daring gratis atau sesi pengetahuan antar-departemen - idealnya keduanya. "Sangat sering ketika orang non-teknis membaca artikel teknis secara online, jargon teknis cenderung tidak menarik," kata Nair. "Memiliki individu di dalam departemen atau organisasi untuk hanya membantu Staf IA melalui pemahaman jargon dan konsep teknologi semacam itu cukup membantu dalam hal menciptakan keinginan untuk mengeksplorasi berbagai aspek teknologi."

Namun perlu diingat bahwa ketika “batas minimum” telah ditetapkan, batasan tersebut perlu dinaikkan dalam waktu singkat. Ketika menilai kerangka kerja ini melalui audit, auditor internal perlu fokus tidak hanya pada apakah keterampilan tersebut diajarkan tetapi juga melihat bagaimana keterampilan tersebut diterapkan dan dibangun secara berkelanjutan dan efektif seiring dengan berkembangnya basis pengetahuan.

“Strategi peningkatan keterampilan yang efektif harus mencakup beberapa pengukuran 'kebugaran digital',” kata Nair. “Ukuran kinerja departemen tidak boleh terbatas pada penerapan teknologi; hal ini juga harus mencakup KPI yang mengukur bagaimana departemen terus berkembang sehubungan dengan penggunaan teknologi tertentu. Oleh karena itu, para pemimpin audit internal perlu melakukan advokasi untuk mendukung peningkatan KPI yang menunjukkan bagaimana departemen melakukan transformasi, bukan hanya menerapkan teknologi tertentu. Tanpa evolusi atau transformasi yang berkelanjutan, setiap orang berisiko mengalami stagnasi.”

Pelletier menambahkan, “Teknologi terintegrasi ke dalam segala hal yang kita lakukan, jadi kita harus terus melakukan advokasi untuk meningkatkan standar tersebut. Teknologi terus berubah, jadi kita sudah berada dalam mode mengejar ketertinggalan. Jika kita tidak bergerak, kesenjangan akan terus bertambah. Sebagai pemimpin audit, tujuan Anda adalah mengatur seberapa luas atau sempit keinginan Anda dan dewan direksi untuk mengatasi kesenjangan tersebut.”

Hidup, Raja Data

Landasan Semua Kemajuan Teknologi

Menemukan data berkualitas dan memahaminya

Data adalah raja, kata klise, dan semakin hari semakin benar. Apa pun strategi yang digunakan untuk menciptakan tim digital yang efektif, tidak ada satupun yang akan memberikan hasil tanpa akses terhadap data berkualitas.

“Data sangat penting untuk mengaudit pekerjaan, terutama dengan penggunaan sistem dan kontrol otomatis yang berlaku,” kata Wong. “Mengingat banyaknya data saat ini, peluang untuk memanfaatkannya dalam audit internal sangat besar – asalkan orang tersebut tahu cara menggunakannya, sehingga kekurangan data menjadi semakin bermasalah.”

Meskipun kita menyadari bahwa kekurangan data merupakan sebuah permasalahan, bahkan saat ini, akses terhadap data berkualitas masih belum bisa diterima. Hal yang sama mengkhawatirkannya, kata Nair, adalah ketika departemen IA menggunakan persepsi ketidakmampuan mereka memperoleh data sebagai alasan untuk tidak melakukan penerapan teknologi dalam aktivitas IA. Hal ini tidak mungkin terjadi. Sebaliknya, perjalanan untuk memperoleh dan memanfaatkan data harus digunakan sebagai bagian penting dari kasus bisnis audit internal untuk kemajuan teknologi. “Dalam hal integritas data, fungsi IA tidak boleh membatasi diri hanya pada identifikasi atau kategorisasi data baik atau buruk,” ujarnya. “Sebaliknya, fungsi-fungsi IA harus memanfaatkan peluang ini untuk menyampaikannya kepada manajemen eksekutif, memberikan rekomendasi untuk meningkatkan kualitas data, dan menjalankannya. Menghentikan penggunaan teknologi dalam audit karena permasalahan tersebut dapat mengakibatkan fungsi IA tidak bergerak maju dalam upaya teknologinya.”

Hal ini tidak mungkin terjadi. Sebaliknya, perjalanan untuk memperoleh dan memanfaatkan data harus digunakan sebagai bagian penting dari kasus bisnis audit internal untuk kemajuan teknologi. “Apa yang kami lihat adalah kita tidak boleh selalu membatasi diri hanya dengan mengidentifikasi apakah data itu baik atau buruk,” ujarnya. “Sebaliknya, kita harus benar-benar bergerak maju, menyorotinya, dan menggunakannya sebagai cara untuk mengidentifikasi area yang perlu ditingkatkan, berkomunikasi dengan manajemen, dan menjaga agar upaya tetap berjalan. Karena jika kita berhenti pada titik tertentu, hal itu berisiko menjadi stagnan selamanya.”

Data tidak selalu memerlukan investasi untuk pengumpulannya. Sering kali, yang penting hanyalah memiliki pengetahuan untuk memanfaatkan data yang sudah ada. Bahkan informasi yang dilacak dalam *spreadsheet Excel* dapat dianggap sebagai data berkualitas tergantung pada situasinya. Kunci untuk membukanya sederhana: keterampilan yang tepat untuk memperhatikan dan menyorotinya serta memanfaatkannya, dan budaya yang tepat untuk mendorong pengembangan keterampilan tersebut. Dengan kata lain, di mana bakat dipupuk dan dikembangkan, data akan mengikuti.

Dalam lingkungan yang tepat, data tidak harus benar-benar ideal untuk dianggap berharga. “Menurut saya, memiliki data selalu lebih baik daripada tidak memiliki data apapun,” kata Wong. “Bahkan kumpulan data yang tidak lengkap masih lebih baik daripada tidak memiliki data sama sekali. Hal yang lebih penting daripada kelengkapan data adalah memiliki pola pikir untuk memanfaatkan setiap peluang analisis data dari apa yang Anda miliki. Katakanlah saya memberi Anda $10, tetapi saya memberikannya kepada Anda dalam bentuk sen. Anda akan tetap menerimanya dengan dasar bahwa harganya masih $10, meskipun itu agak rumit.”

Namun, audit internal harus melakukan lebih dari sekedar memahami bagaimana data digunakan. Menurut Pelletier, pengetahuan data bertujuan untuk menjawab empat pertanyaan:

- Dari mana asalnya?

- Dimana disimpannya?
- Apa yang dilakukan terhadap data tersebut?
- Bagaimana cara membuang atau menghancurkannya?

Umumnya, menjawab pertanyaan-pertanyaan ini tidak memerlukan pengetahuan teknis tingkat tinggi.

"Tata kelola data adalah sesuatu yang saya pikir setiap auditor harus menjadi ahli," kata Pelletier. "Beberapa aspek mungkin memerlukan pengetahuan teknis yang lebih dalam, tetapi setiap auditor harus dilengkapi pengetahuan untuk dapat mengajukan pertanyaan yang menantang dan memahami proses yang mendasarinya dan menarik keahlian teknis hanya pada bagian-bagian yang Anda butuhkan."

Kesimpulan

Teknologi adalah peluang, bukan kerugian

Terlepas dari semua perbincangan tentang manfaat luar biasa yang dapat diberikan oleh teknologi, hal ini juga dapat menimbulkan kekhawatiran yang sama besarnya. Wajar jika kita menganggapnya sebagai sesuatu yang membebani – bahkan sampai pada titik dimana seseorang mungkin mulai mempertanyakan keamanan kerja mereka sendiri. Pada titik tertentu seiring berkembangnya teknologi, apakah akan ada tempat bagi pekerjaan manusia?

Hal ini merupakan kekhawatiran yang dapat dimengerti, namun kekhawatiran ini berasal dari budaya organisasi yang salah. Teknologi tidak boleh dipandang sebagai pesaing atau ancaman — teknologi harus dipandang dengan antusias sebagai peluang untuk mencapai lebih banyak hal, memberikan nilai lebih kepada organisasi, dan bahkan meningkatkan kinerja sehari-hari setiap pekerja.

“Meskipun bukan mayoritas, mungkin masih ada sejumlah orang yang percaya bahwa otomatisasi akan menghilangkan pekerjaan mereka atau mereka yang secara perilaku cenderung mempertahankan cara mereka sendiri dalam melaksanakan audit, seperti melakukan apa yang Anda sukai, katakanlah penggunaan *spreadsheet* lama yang bagus,” kata Nair. “Para pemimpin IA harus mendorong diskusi tentang perlunya untuk tetap tangkas di era dinamis yang didorong oleh teknologi ini, dengan mengadopsi pola pikir pembelajaran dan potensi manfaat teknologi, terutama yang dirancang sebagai sarana untuk mengurangi beban kerja departemen atau meningkatkan efisiensi, bukan sebagai sarana untuk menggantikan auditor. ”

"Meskipun bukan mayoritas, mungkin masih ada sejumlah orang yang percaya bahwa otomatisasi akan mengambil pekerjaan mereka atau mereka yang secara perilaku memilih untuk mempertahankan cara mereka sendiri dalam melaksanakan audit, seperti melakukan apa yang dirasa nyaman, misanyal menggunakan kertas kerja lama yang telah familiar," kata Nair. "Para pimpinan IA harus mendorong diskusi tentang perlunya tetap gesit di era teknologi yang dinamis ini, menerapkan pola pikir pembelajar dan potensi manfaat teknologi, terutama yang diarahkan untuk mengurangi beban kerja departemen atau meningkatkan efisiensi, bukan sebagai pengganti auditor.”

Audit internal dapat dan harus menjadi pendukung terbesar teknologi dalam organisasi. Ia adalah pembawa perubahan, mitra, dan pembawa kabar baik. Ketika tantangan teknologi terus berlanjut, organisasi dapat memakai teknologi tersebut lebih banyak lagi.

Tentang IIA

The Institute of Internal Auditors (IIA) adalah sebuah asosiasi profesional internasional nirlaba yang melayani lebih dari 235.000 anggota global dan telah memberikan lebih dari 190.000 sertifikasi Certified Internal Auditor (CIA) di seluruh dunia. Didirikan di tahun 1941, The IIA dikenal di seluruh dunia sebagai pemimpin profesi audit internal dalam standar, sertifikasi, pendidikan, penelitian, dan bimbingan teknis. Untuk informasi lebih lanjut, kunjungi theiia.org.

Tentang Wolters Kluwer TeamMate

Wolters Kluwer TeamMate Audit Management Solutions adalah solusi ahli audit dan asurans internal terkemuka di dunia dengan lebih dari 25 tahun didedikasikan untuk memajukan auditor korporat, komersial, dan sektor publik. Seiring dengan berkembangnya tim audit internal untuk memberikan wawasan yang lebih mendalam, asurans risiko yang lebih besar, dan meningkatkan efisiensi, mereka memerlukan solusi yang mempunyai tujuan dan siap menghadapi masa depan. TeamMate memberikan solusi ahli yang diandalkan oleh auditor internal untuk mendorong nilai ke dalam organisasi mereka. Untuk informasi lebih lanjut, kunjungi www.teammatesolutions.com.

Disclaimer

Hak Cipta

Mei 2024

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101